UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/798,070	03/11/2004	Stefan G. Hild	CH920020049US1	5669

54856 7590 01/12/2006

LOUIS PAUL HERZBERG
3 CLOVERDALE LANE
MONSEY, NY 10952

EXAMINER	
WANG, JIN CHENG	
ART UNIT	PAPER NUMBER
2672	

DATE MAILED: 01/12/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/798,070	**Applicant(s)** HILD ET AL.
	Examiner Jin-Cheng Wang	**Art Unit** 2672

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 28 November 2005.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-20 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-20 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

Applicant's submission filed on 11/28/2005 has been entered. Claims 16-20 have been newly added. Claims 1-20 are pending in the application.

Response to Arguments

Applicant's arguments filed November 28, 2005 have been fully considered but are not found persuasive in view of the ground(s) of rejection set forth below.

As address below, the claim 1 is anticipated by **S. Ma, et al., "EventMiner: An integrated mining tool for Scalable Analysis of Event Data", May 21, 2001, www.research.ibm.com**.

Applicant argues that applicant's apparatus and system for monitoring events in a computer network enabling an operator of an intrusion-detection system to simultaneously monitor various event attributes versus the arrival time of the events. However, "the apparatus and system...to simultaneously monitor various event attributes" cannot be found as a claim limitation in the claim 1 because the claim 1 only recites the viewing of the primary attribute and the multiple attribute values of the primary attribute are viewed on the same display. Nowhere in the claim 1 recites a secondary attribute being viewed together with the primary attribute on the same display. Although multiple attribute values related to the primary attribute can be presented on the same display, there is a fundamental difference between the attribute values for one attribute and the attribute values for another attribute. Moreover, it is not ascertained from the claim invention set forth in the claim 1 whether the claim limitation of "attributes" refer to event attributes, pattern attributes or the data attributes. Applicant failed to particularly point out and distinctly claim the subject matter which applicant regards as invention.

Applicant also argues that there is apparently no indication that Ma performs a step of determining a primary attribute" as in claim 1. However, the cited prior art teaches in Fig. 7 and the last paragraph of the Page 12 plotting the primary attribute (e.g., with the attribute values indicating the troublesome hosts having significantly high event counts) versus time with the attribute values for events in a communication network and the primary attribute is selected from a plurality of attributes related to the one or more significant measurements such as the co-occurrences (i.e., the total number of times that two hosts generate events within a predefined time window), the conditional probability of the two hosts (i.e., the probability of a host generating an event given the observation that the other host has generated an event), the chi-squared test and so on. Fig. 4 shows the coloring of the events having the primary attribute with the patterns indicating the authentication failure and SNMP request in order to differentiate using the coloring the events with authentication failure from other events. A pattern label is assigned to the events falling into the same pattern. Finally, the operator can view different event attributes by switching menus (Fig. 6).

Applicant argues that, "the cited reference, S. Ma, et al., indeed presents other event mining methods. That visualization method using a two-dimensional mapping technique of arbitrary event attributes versus arrival time enabling an operator to analyze the event history. A distinct disadvantage of this method is that only one of the event attributes may be plotted versus the arrival time of the events. Thus, the operators have to switch continuously between the various event attributes to make sure that they do not miss a significant event pattern. The disadvantages of S. Ma et al., are overcome with the invention claimed in claims 1-15." The Examiner respectfully disagrees with the applicant's remarks because applicant's statement, "only one of the event attributes may be plotted versus arrival time of the events", is incorrectly construed. As previously addressed, Ma has taught in Fig. 7 and the last paragraph of the Page 12 plotting the primary attribute (e.g., with the attribute values indicating the troublesome hosts having significantly high event counts) versus time with the attribute values for events in a communication network. Ma has also taught a plurality of attributes related to the one or more significant measurements such as the co-occurrences (i.e., the total number of times that two hosts generate events within a predefined time window), the conditional probability of the two hosts (i.e., the probability of a host generating an event given the observation that the other host has generated an event), the chi-squared test and so on wherein the attribute values are plotted in the same plot. It is clear that Ma discloses attributes including categorical attributes of the hosts, event types, severity of the events, etc. See Figs. 2, 6, 7 and 9.

Applicant's statement, "the operators have to switch continuously between the various event attributes to make sure that they do not miss a significant event pattern," is incorrect. This is because in Ma many significant event patterns are simultaneously identified within a single plot without the operator's switching between the various event attributes.

Applicant argues that, "although Ma has a display, Ma apparently do not allocate a display label to the events indicating the attribute values of the primary attribute." It is noted that the claim 1 requires "a display label to the events indicating the attribute values of the primary attribute." However, Ma discloses display label to the events such as "Link down of host A", "node down of host B", "authentication failure of host A", etc., including the colors for coloring the different patterns that indicate the attribute values of the primary attribute such as the co-occurrences of some specific events within a predefined time window.

Applicant also argues that, "although Ma has a display, Ma apparently do not have a second display." This argument does not make sense, because the claim 1 set forth "a second display label" which is different from the meaning of "a second display." Applicant's claim 1 recites "a second display label". However, Ma discloses display label including the colors for coloring the different patterns for the events in the communication network that indicate the attribute values of the primary attribute such as the co-occurrences of some specific events within a predefined time window.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-20 are rejected under 35 U.S.C. 102(b) as being anticipated by S. Ma, et al., "EventMiner: An integrated mining tool for Scalable Analysis of Event Data", May 21, 2001, www.research.ibm.com.

Claim 1:

Ma teaches a method of monitoring events in a computer network, the method comprising:

Said computer network triggering said events, each event being provided with attribute values allocated to a given set of attributes (*The term "attributes" are not clear as it may be related to the data object attributes for each event or the pattern attributes for each pattern for a plurality of data objects*; *However, the pattern attributes for a plurality of data objects are also related to the data object attributes as a pattern is computed from the plurality of data objects. The cited reference teach mapping a plurality of data attributes to item to identify correlations across different hosts and event types by using the mapping that maps the pair of event type and host name to item and leaves key empty. See Page 11. Moreover, the cited reference in Page 1, second paragraph, explicitly teaches the attribute values, see the last paragraph of Page 6 and the first and second paragraphs of Page 8, the last paragraph of Page 12, and* ***the real data set*** *collected from a production computer network containing thousands of managed nodes including routers, hubs and servers are described in the last paragraph of page 3 and identifying unknown event patterns that can be used for real-time monitoring is described in the second paragraph of page 3. Ma has also taught* ***a plurality of pattern attributes related to the one or more significant measurements such as the co-occurrences,*** *i.e., the total number of times that two hosts generate events within a predefined time window, the conditional probability of the two hosts, i.e., the probability of a host generating an event given the observation that the other host has generated an event, the chi-squared test and so on*);

Providing an event display with a cross plot having x and y coordinate axes, the x-axis presenting a time period and the y-axis present an attribute value range (*e.g., The cited reference teach mapping a plurality of data attributes to item to identify correlations across different hosts and event types by using the mapping that maps the pair of event type and host name to item and* *leaves key empty. See Page 11. Figs. 2, 4, 6, 7, 9 and the third paragraph of Page 8 describes a scatter plot or cross plot having an y-axis representing around 160 hosts of a communication network and the x axis has been described in the figures as well as the first paragraph of page 6; for attribute value range, see these figures as well as the description in the second paragraph of Page 8*);

Determining a primary attribute of the events selected from the given set of attributes to be presented with its attribute values on the y-axis of the cross plot (*e.g., The cited reference teach mapping a plurality of data attributes to item to identify correlations across different hosts and event types by using the mapping that maps the pair of event type and host name to item and leaves key empty. The attributes including the categorical attributes or temporal attributes and the primary attribute values are displayed in Figs. 2, 4, 6 and 7 and multiple attributes are described in the last paragraphs of Page 11 and 12*),

Allocating a first display label (*e.g., one of the colors indicating the patterns such as the Pattern 1, Pattern 2, Pattern 3 and Pattern 4 as marked in the scatter plot or the cross plot of Figs. 2, 6, 7 and 9 such as "Link down of host A" and "node down of host B"*) to the events (*e.g., alarms in Page 10*) indicating (*mapping of the attributes wherein the mapping results are shown in the plots with the patterns identifying/indicating the attribute values of the primary attribute related to the categorical attribute such as the host A or the host B. Moreover, the pattern attribute values identifying the pattern 1 and the pattern 2 also describe the primary attribute such as the host A and the host B for the patterns such as "Link down of host A" and "node down of host B"*) the attribute values of the primary attribute (*e.g., co-occurrence of certain events or the categorical attribute and event type associated with the events wherein the* *primary attribute is related to the primary attribute of the data set or the primary attribute of the patterns; See Page 12 and the key attribute values are described in the second paragraph of page 3*), providing a pattern algorithm (*the pattern algorithm is described in Fig. 7 as well as the mining algorithm as described in the last paragraph of page 12 or the EventMiner for* *<u>ordering categorical values</u>* *wherein the event generating, say every 300 seconds, may be identified*) to detect whether an arrived event (*arrived event are the selected event objects or the selected data objects in a specific time range related to the events progressively loaded from a database or the mining alarm logs in a real time system; see first paragraph of page 13 and the last paragraph of page 10 and a new query that retrieves the relevant data objects for more analysis in which a new query is restricted to a range constraint for a numerical attribute; see the last paragraph of page 10*) is part of the given pattern (*is part of the given pattern such as the Pattern 1 or the Pattern 2 from the identifiable patterns such as the* ***SNMP request, authentication failure, link up, link down, port up, port down*** *wherein authentication failure indicates a possible security intrusion and* ***<u>link down of host A indicates the attribute associated with the data objects as well as the attribute associated with the event</u>***) on the basis of a comparison of the attributes allocated to the given pattern and of the attributes assigned to the arrived event (*e.g., the co-occurrence measurements for events can be computed for the data sets or the data objects and the temporal correlation with the selected hosts from the other side of the AttributeViewer can be identified using the color linkage by the coloring and filtering algorithm or the data mining algorithm in which the difference or similarity in terms of patterns indicated by colors is compared; see page 12-13*), providing a mapping algorithm to map any attribute value of an attribute selected from the given set of attributes onto the y-axis of the cross plot (*see the last* *paragraphs of Page 11-12; The cited reference teach mapping a plurality of data attributes to item to identify correlations across different hosts and event types by using the mapping that maps the pair of event type and host name to item and leaves key empty.*),

Allocating a second display label (*e.g., one of the colors indicating the patterns such as the Pattern 1, Pattern 2, Pattern 3 and Pattern 4 as marked in the scatter plot or the cross plot of Figs. 2, 6, 7; SNMP request, authentication failure, link up, link down, port up, port down wherein authentication failure indicates a possible security intrusion may be used as display labels as well. The attribute values may be used as display labels as well*) to the events indicating the attribute values of the attributes being uncovered (*discovered*) as part of the given pattern (*e.g., the co-occurrence measurements for events can be computed and the temporal correlation with the selected hosts from the other side of the AttributeViewer can be identified using the color linkage by the coloring and filtering algorithm or the data mining algorithm in which the difference or similarity in terms of patterns indicated by colors is compared; see page 12-13; the display labels indicate the attribute values of the attributes being discovered as part of the given pattern, for example, the second host was near a critical level for a key metric indicates the attribute values of the attributes being discovered as part of the given pattern)*, plotting all the events arrived within the time period and including an attribute value allocated to the primary attribute into the cross plot with the first display label indicating the primary attribute, the position of the first display label of each event in the cross plot being determined on the basis of the attribute value of the primary attribute of the event and its arrival time (*e.g., The cited reference teach mapping a plurality of data attributes to item to identify correlations across different hosts and event types by using the mapping that maps the pair of event type and host* *name to item and leaves key empty. Figs. 2, 4, 6, and 7 and the related paragraphs mentioned above in "allocating a first display label". e.g., one of the colors indicating the patterns such as the Pattern 1, Pattern 2, Pattern 3 and Pattern 4 as marked in the scatter plot or the cross plot of Figs. 2, 6, 7; SNMP request, authentication failure, link up, link down, port up, port down wherein authentication failure indicates a possible security intrusion may be used as display labels as well. The attribute values may be used as display labels as well*), and

Plotting the all events arrived within the time period (*Figs. 2, 4, 6, and 7 plot the all events within a specific time range*) and being detected by means of the pattern algorithm (*by the event miner algorithm*) as part of the given pattern into the cross plot with the second display label (*e.g., one of the colors indicating the patterns such as the Pattern 1, Pattern 2, Pattern 3 and Pattern 4 as marked in the scatter plot or the cross plot of Figs. 2, 6, 7 and 9 or Pattern 2 or the Green Spike in Fig. 10*), the position of the second display label of each event in the cross plot being determined by the mapping algorithm on the basis of the attribute value of the attribute of the event (*see Figs. 1-10*) on the basis of the attribute value of the attribute of the event being uncovered (*uncovered for example in the alarm log and uncovered by the mining algorithm*) as part of the given pattern and its arrival time (*discovered as part of the given pattern such as Patterns 1-4 and its arrival time; all the selected events are in a specific time range as plotted in Figs. 2, 4, 6, 7 and 10*).

In other words, Ma discloses an apparatus and system for monitoring events in a computer network enabling an operator of an intrusion-detection system to simultaneously monitor various event attributes versus the arrival time of the events, for example, authentication failure indicates a possible security intrusion may be used as display labels. The cited prior art teaches in Fig. 7 and the last paragraph of the Page 12 plotting the primary attribute (e.g., with the attribute values indicating the troublesome hosts having significantly high event counts) versus time with the attribute values for events in a communication network and the primary attribute for a host is selected from a plurality of attributes related to the categorical values, the one or more significant measurements such as the co-occurrences (i.e., the total number of times that two hosts generate events within a predefined time window), the conditional probability of the two hosts (i.e., the probability of a host generating an event given the observation that the other host has generated an event), the chi-squared test and so on.

Fig. 4 shows the coloring of the events having the primary attribute with the patterns indicating the authentication failure and SNMP request in order to differentiate using the coloring the events with authentication failure from other events. A pattern label is assigned to the events falling into the same pattern. Finally, the operator can view different event attributes by switching menus (Fig. 6).

Ma has taught in Fig. 7 and the last paragraph of the Page 12 plotting the primary attribute (e.g., with the attribute values indicating the troublesome hosts having significantly high event counts) versus time with the attribute values for events in a communication network. Ma has also taught a plurality of attributes related to the one or more significant measurements such as the co-occurrences (i.e., the total number of times that two hosts generate events within a predefined time window), the conditional probability of the two hosts (i.e., the probability of a host generating an event given the observation that the other host has generated an event), the chi-squared test and so on wherein the attribute values are plotted in the same plot. See Figs. 2, 6, 7 and 9. Many significant event patterns are simultaneously identified within a single plot without the operator's switching between the various event attributes.

Ma discloses display label including the colors for coloring the different patterns that indicate the attribute values of the primary attribute such as the co-occurrences of some specific events within a predefined time window.

Re Claims 2-3:

Ma further discloses selecting the new events within the specified time period and plotting the new events within the shifted time period into the cross plot. See Figs. 6, 7, 9 and 10 in which events in the two time periods are drawn and the spikes are identified and the newly selected events are redrawn as determined by the data mining algorithm for the time period during which the new events are retrieved. The database records the attribute values and the arrival time of a new event. The pattern algorithm determines on the basis of the recorded attribute values of event whether or not the newly arrived event in the database and the newly retrieved event from the database includes an attribute value of the primary attribute, for a certain host and event type, as determined the pattern algorithm using the mapping mechanism for mapping a plurality of attributes including the primary attribute into an item for presentation, and the pattern algorithm also determines if the newly arrived event, e.g., alarm, includes the attribute value for the primary attribute, e.g., a certain host or a certain event type including *SNMP request, authentication failure, link up, link down, port up, port down, link down of host A, node down of host B etc.*, shifting the x-axis of the cross plot for the new time period so that the new time period being presented on the x-axis covers the arrival time of the event and plotting the event arrived within the shifted time period into the cross plot with the first display label indicating the primary attribute.

Ma discloses determining on the basis of the recorded attribute values of event from the alarm log or the database whether or not the newly arrived event for the new time period is part of the given pattern using the pattern algorithm on the basis of a comparison of the attributes allocated to the given pattern, for example a composite pattern of Page 13, on the basis of a comparison analysis, and of the attribute assigned to the arrived event wherein the newly arrived event are determined by the retrieval time ranges and data ranges including the host names and types from the database. Ma further discloses determining if the newly arrived event includes an attribute value of the given pattern including the mutual dependence measurement of an m-pattern adding the event to the previous events being detected as part of the given pattern, and redrawing all the events being associated with given pattern in the cross plot by updating the cross plot.

Re Claims 4-5:

Ma further discloses the third display label and the fourth display label indicating the new patterns (See the three colored spikes in Fig. 6 and the four patterns in Fig. 7).

Ma discloses determining if the newly arrived event does not include an attribute value of the given pattern, on the basis of the recorded attribute values of all previous arrived events from the alarm logs or from the database, by means of the mining algorithm whether or not the newly arrived event is part of a new pattern on the basis of a comparison (Page 13) of the attributes allocated to the new pattern and of the attributes assigned to the arrived events. Ma discloses allocating a third display label to the events, including the coloring of the new pattern, indicating the attribute values of the attributes being discovered as part of the new pattern wherein a large amount of patterns can be discovered by the mining algorithms. Ma discloses plotting the all events being detected by means of the mining algorithm as part of the new pattern into the cross plot with the third display label indicating the new pattern, the position of the third display label of each event in the cross plot being determined by the mapping algorithm (Page 12 for the mapping of the attributes into item and thereby determining the positions of the patterns on the cross plot) on the basis of the attribute value of the attribute of the event (event types, host names etc) being uncovered as part of the new pattern, such as *SNMP request, authentication failure, link up, link down, port up, port down, link down of host A, node down of host B etc*, and its arrival time in the database.

Ma discloses removing all the events including an attribute value allocated to the primary attribute from the cross plot, if a primary attribute to be presented with its attribute values on the y-axis of the cross plot is changed (if the mapping mechanism for mapping a plurality of attributes including the host names and event types are changed), allocating a fourth display label including *SNMP request, authentication failure, link up, link down, port up, port down, link down of host A, node down of host B etc*, to the events indicating the attribute values of the new primary attribute (e.g., category attribute, event type of data objects). Ma discloses plotting all the events arrived within the time period as retrieved from the database and including an attribute value allocated to the new primary attribute into the cross plot with the fourth display label, including *SNMP request, authentication failure, link up, link down, port up, port down, link* *down of host A, node down of host B etc, indicating the new primary attribute,* such as the host name and event type, the position of the fourth display label of each event in the cross plot being determined by the mapping mechanism in Page 12 on the basis of the attribute value of the primary attribute of the event and its arrival time as determined by the retrieval condition from the database.

Re Claim 6:

Ma further discloses the operator selects the events to be plotted and displaying textual and coloring information associated with the selected events on the event display (Page 4 and Figs. 6, 7, 9-10).

Ma discloses plotting all attribute values, including the attributes such as event type, link down, and host name, host A, in the patterns marked as the link down of host A, node down of host B, recorded for an event, as retrieved from the database, with the respective display label into the cross plot if the event is selected by an operator and displaying textual information associated with the selected event on the event display.

Re Claim 7:

Ma further discloses a pattern algorithm such as the data mining algorithm suitable to perform multi-attribute pattern recognition (Figs. 6, 7, 9-10).

Ma discloses the mining algorithm being suitable to perform multi-attribute pattern recognition using the mapping mechanism (Page 12) and the pattern comparisons/matching (Page 13).

Re Claim 8:

Ma further discloses using color such as Red and Green to color the pattern Spikes and Pattern 1, Pattern 2, Pattern 3, Pattern 4 for specific mark layouts (Figs. 6, 7, 9-10).

Ma discloses each display label includes different colors marking the events.

Re Claim 9:

Ma further discloses all events being uncovered as part of the pattern being clustered by the display label such as Red Spikes, Green Spikes (Figs. 6, 7 and 9-10).

Ma discloses all events being discovered as part of the pattern as clustered by the different labels including Red Spikes and Green Spikes to indicate one of the plurality of events such as *SNMP request, authentication failure, link up, link down, port up, port down, link down of host A, node down of host B etc, indicating the new primary attribute.*

Re Claim 10:

Ma further discloses a data mining algorithm and GUI (Page 14). Ma discloses the mining algorithm carrying the steps as recited in the claim 1.

Re Claim 11:

Ma further discloses the program code being stored on data carrier (see page 5). Data carrier is inherent within the computer embodiment of Page 5.

Re Claim 12:

Ma further discloses an event visualization device for monitoring events in a computer network (Page 3). *The cited reference teach mapping a plurality of data attributes to item to identify correlations across different hosts and event types by using the mapping that maps the pair of event type and host name to item and leaves key empty. See Page 11. Moreover, the cited reference in Page 1, second paragraph, explicitly teaches the attribute values, see the last paragraph of Page 6 and the first and second paragraphs of Page 8, the last paragraph of Page 12, and **the real data set** collected from a production computer network containing thousands of managed nodes including routers, hubs and servers are described in the last paragraph of page 3 and identifying unknown event patterns that can be used for real-time monitoring is described in the second paragraph of page 3.*

Re Claims 13-15:

Ma further discloses an implementation of the Event Miner algorithm on the computer (Page 4-5).

Claim 16:

The claim 16 is subject to the same rationale of rejection set forth in the claims 2-4.

Claim 17:

The claim 17 is subject to the same rationale of rejection set forth in the claim 5.

Claim 18:

The claim 18 is subject to the same rationale of rejection set forth in the claims 2-4.

Claim 19:

The claim 19 is subject to the same rationale of rejection set forth in the claim 5.

Claim 20:

The claim 20 is subject to the same rationale of rejection set forth in the claim 11.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jin-Cheng Wang whose telephone number is (571) 272-7665. The examiner can normally be reached on 8:00 - 6:30 (Mon-Thu).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Mike Razavi can be reached on (571) 272-7664. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

jcw

MICHAEL RAZAVI
SUPF [illegible] INER
[illegible] 00